Redmine - Defect #34367

Allowed filename extensions of attachments can be circumvented

2020-12-02 15:13 - Holger Just

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Attachments	**Estimated time:**	0.00 hour
Target version:	4.0.9		
Resolution:	Fixed	**Affected version:**	

Description

In #20008, Redmine introduced the ability to restrict the allowed extensions of attachment filenames.

This check is not exhaustive though, meaning it is easily possible to subvert the restriction. There are two ways how a user can still use any arbitrary filename despite restrictions in place:

- As reported by Bartu Ogur via email to security@redmine.org, it is also possible to update the filename of an uploaded attachment when it is attached to an object. The filename of the original file is checked here only during attachments#upload when the attachment is initially created. However, we do allow to overwrite the filename (and content type) of an attachment when it is attached to an object in redmine:source:trunk/lib/plugins/acts_as_attachable/lib/acts_as_attachable.rb#L105.
- Furthermore, after an attachment was initially added with an allowed extension and was successfully attached to an object, the filename can be edited freely to set any filename, including with a forbidden extension.

For administrators trying to restrict the types of files which can be uploaded, these limitations are not obvious, making the usage of this feature potentially dangerous (also with Redmine relying on the extension to determine the content type in a lot of areas).

To fix the reported issue and to enforce the filename everywhere on change, we could use the attached patch against current trunk. With this patch, each change of the filename will be validated against the list of allowed attachments. This will remove the ability to set a currently forbidden extension to any file, regardless on when it was created.

Associated revisions

Revision 20946 - 2021-04-16 03:36 - Go MAEDA

Validate attachment filenames on every change (#34367).

Patch by Holger Just.

Revision 20947 - 2021-04-16 03:44 - Go MAEDA

Merged r20946 from trunk to 4.2-stable (#34367).

Revision 20948 - 2021-04-16 03:45 - Go MAEDA

Merged r20946 from trunk to 4.1-stable (#34367).

Revision 20952 - 2021-04-20 01:43 - Go MAEDA

Merged r20946 from trunk to 4.0-stable (#34367).

History

#2 - 2021-04-14 19:31 - Holger Just

bump.

#3 - 2021-04-15 04:52 - Go MAEDA

- Status changed from New to Confirmed

- Target version set to 4.1.3

Confirmed the issue. Setting the target version to 4.1.3.

#4 - 2021-04-16 03:45 - Go MAEDA

- Status changed from Confirmed to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch. Thank you for handling this issue.

#5 - 2021-04-16 14:09 - Holger Just

Thank you!

#6 - 2021-04-19 23:06 - Marius BĂLTEANU

- Status changed from Closed to Reopened

- Target version changed from 4.1.3 to 4.0.9

#7 - 2021-04-23 06:53 - Go MAEDA

- Status changed from Reopened to Resolved

#8 - 2021-04-26 18:19 - Marius BĂLTEANU

- Status changed from Resolved to Closed

#9 - 2021-04-28 10:25 - Holger Just

CVE-2021-31865 has been assigned for this.

#10 - 2022-06-21 08:12 - Marius BĂLTEANU

- Project changed from 2 to Redmine

- Category set to Attachments

Files

0001-Validate-attachment-filenames-on-every-change.patch	3.04 KB	2020-12-02	Holger Just